

Envoria - Technical and Organizational Measures

– Pursuant to Article 32 GDPR –

Table of Contents

1. Introduction	3
2. The SaaS Solution	3
3. Technical and Organizational Measures	4
a. Physical Access Control	4
b. System Access Control	5
c. Data Access Control	5
d. Separation Control	6
e. Pseudonymization and Encryption	6
f. Transmission Control	6
g. Input Control	7
h. Availability Control	7
i. Resilience	7
j. Review, Assessment and Evaluation	8
k. Order Control	9

1. Introduction

The Processor ensures a level of protection appropriate to the specific processing activity. This is described as follows:

Processing of data on behalf of the Controller in accordance with instructions is ensured through the technical and organizational separation of responsibilities between the Controller and the Processor. Processing of data on behalf of the Controller only takes place in exceptional cases, for example through services relating to system setup, support, training, programming, or troubleshooting of program functions..

2. The SaaS Solution

To operate its cloud infrastructure, Envoria relies on established data center and cloud service providers. The hosting environment is operated within modern, cloud-based data centers, which are provided by Exoscale when using Envoria, and by Hetzner Online GmbH when using Envoria Lease Accounting. This infrastructure is located within the European Union or in countries covered by a corresponding adequacy decision of the European Commission.

Further details on the security standards and measures of the cloud providers can be found on the official security pages of [Exoscale](#) and [Hetzner Online GmbH](#).

3. Technical and Organizational Measures

The Processor implements the following technical and organizational measures to ensure data security within the meaning of Art. 32 GDPR. The effectiveness of these measures is regularly reviewed, assessed, and further developed.

a. Physical Access Control

Measures that prevent unauthorized persons from gaining physical access to facilities in/with which personal data is processed or used.

Technical Measures	Organizational Measures
→ The Processor's business premises are located in an office building. The entrance door is secured by a locking system. → Access to the data center is logged, monitored, and traceable	→ Introduction of access authorizations for employees and third parties, including corresponding documentation → Access to the building is staffed by reception personnel → Mandatory visitor registration → Visitors are only permitted when accompanied by an employee → Security personnel outside regular business hours → Careful selection of cleaning staff → Immediate revocation of access authorizations when employees or service providers leave

b. System Access Control

Measures that prevent unauthorized persons from using data processing systems.

Technical Measures	Organizational Measures
→ Physical deletion of data carriers prior to reuse → Login using username, password and, where applicable, two-factor authentication (2FA) → Login using biometric data → Automatic desktop lock → Hard drive/system encryption of mobile devices	→ Creation of an authorization concept by the system administrator → Password policy including password length and complexity requirements → Secure storage of data carriers → Proper destruction of data carriers → Management of user authorizations → Creation of user profiles → Policy for secure passwords → Policy for the deletion and destruction of data → Clear desk and clear screen policy → Instructions for manually locking the desktop → Immediate suspension of user accounts when employees leave

c. Data Access Control

Measures ensuring that authorized persons only have access to personal data for which there is an operational need.

Technical Measures	Organizational Measures
→ Access to the data is protected by differentiated authorizations. → Authentication using username/password → Automatic logout after a period of inactivity; resumption requires re-identification and password entry by the user → Use of anti-virus software, a software firewall and, where applicable, VPN technology → Logging of access	→ Assignment of user rights and user profiles, and allocation of passwords → Use of authorization concepts → Granting of access rights according to the need-to-know principle

d. Separation Control

Measures ensuring that data collected for different purposes is processed separately.

Technical Measures	Organizational Measures
→ Physically separate storage on separate systems or data carriers → Separation of production and test systems	→ Creation of an authorization concept → Control via authorization concept → Logical separation of customer data by tenant

e. Pseudonymization and Encryption

Personal data is processed in such a way that, without the use of additional information, it can no longer be attributed to a specific data subject.

Technical Measures	Organizational Measures
→ Encryption of hard drives using standard Windows tools. → Data transmitted over the internet is always encrypted using current, state-of-the-art technical methods → Encryption of backups	→ Pseudonymization is not applied, as the original data is required in order to reproduce and understand an error in the software application(s) under realistic conditions. → Internal instruction to anonymize or pseudonymize personal data wherever possible in the event of disclosure or after expiry of the statutory retention period.

f. Transmission Control

Measures ensuring that personal data cannot be read, copied, modified, or deleted without authorization during transmission, storage, or transport on external data carriers.

Technical Measures	Organizational Measures
→ Establishment of leased lines or VPN tunnels only together with the Controller → Email encryption → Logging of access → Provision via encrypted connections such as HTTPS	→ Documentation of data recipients and the duration of planned deletion periods → Careful selection of transport routes → Careful selection of personnel → Confidentiality/non-disclosure agreements with external recipients of personal data

g. Input Control

Measures that make it possible to subsequently verify whether personal data that has been entered corresponds to the data supplied. Data entry is controlled by logging at system or application level.

Technical Measures	Organizational Measures
→ Only personalized user accounts are used – no generic accounts → Server-level logging (logins, error messages); application-level logging (logins, changes to content/values, error messages)	→ Overview of which programs are used to process which data → Granting of rights to enter, modify, and delete data based on an authorization concept

h. Availability Control

Measures to maintain availability are intended to ensure that the personal data processed remains available even after an incident, so that operations can resume.

Technical Measures	Organizational Measures
→ Fire and smoke detection system in the building → Storage of backup media at 2 geographically separate locations	→ Backup and recovery concept in place → Regular checks of backup procedures → Regular data recovery tests with logging of results → Documented business continuity management (BCM) process

i. Resilience

Measures ensuring the resilience of systems and services in connection with the processing, i.e., their ability to remain stable and operational even under high load, disruptions, or attacks.

Technical Measures	Organizational Measures
→ Redundant IT infrastructure → Automatic scaling of resources	→ Documented business continuity management (BCM) process

j. Review, Assessment and Evaluation

Measures ensuring the ongoing review, assessment, and evaluation of the effectiveness of the technical and organizational measures for guaranteeing the security of processing.

Technical Measures	Organizational Measures
→ Simple exercise of the data subject's right of withdrawal through technical measures	→ The effectiveness of technical protective measures is reviewed regularly or as needed → Appointed Data Protection Officer → Employees are trained and bound to confidentiality/data secrecy → Regular employee awareness training, at least annually → The organization complies with the information obligations under Art. 13 and 14 GDPR → Documentation of security incidents and data breaches → No more personal data is collected than is necessary for the respective purpose → Documented process for reporting data breaches to the supervisory authority and affected data subjects → Regular reviews of the technical and organizational measures

k. Order Control

Measures ensuring that personal data processed on behalf of the Controller is only processed in accordance with the instructions of the Controller.

Technical Measures	Organizational Measures
	→ Prior review of the security measures taken by the Processor and their documentation → Selection of the Processor with due care (particularly with regard to data protection and data security) → Conclusion of the necessary data processing agreements → Written instructions to the Processor → Confirmation that the Processor's employees are bound to data secrecy → Obligation for the Processor to appoint a Data Protection Officer where legally required → Agreement of effective control/audit rights with respect to the Processor → Provisions governing the use of further subcontractors → Ensuring the destruction or return of data upon termination of the contract → Regular monitoring of the processors/subcontractors used with regard to compliance with the agreed security measures